Health Law and Policy Brief

Volume 1 | Issue 1 Article 7

11-25-2013

Federal Efforts to Impose Uniformity on State Health Information Privacy Laws

Joy L. Pritts

Federal Efforts to Impose Uniformity on State Health Information Privacy Laws

*By Joy L. Pritts, J.D.**

Over the last several years, there have been repeated federal efforts to impose uniformity on state health information privacy laws. This article discusses the historical background of state regulation of health information privacy, recent efforts to preempt state health privacy laws, and reasons these efforts are not likely to succeed.

I. Background

The power to regulate health primarily resides with the states. According to the National Governors Association, individual states have regulated the creation and management of medical records for over 150 years.[1] Towards the end of the 20th century, states began to adopt statutory provisions to regulate the confidentiality or privacy of health information, a matter which had previously been primarily addressed through professional ethics. Presently, every state has statutes and regulations governing the use and disclosure of health information.

Beginning in the 1970s, states began passing comprehensive health privacy laws intended to promote patients' full participation in the healthcare system by fostering trust between patients and healthcare providers.[2] These detailed statutes are based on established fair information practice principles. While the respective state statutes are somewhat similar in their core principles of notice, disclosure, secondary use, correction, and security, they often differ in the details, such as the required contents of consent authorization forms.

In response to health needs of their citizens, most states enacted laws to enhance privacy protections for information related to specific medical conditions that are associated with stigmas or discrimination, such as HIV/AIDS or mental health conditions. Generally, these statutes require specific, informed, and written patient authorization before information related to these "sensitive" medical conditions may be shared with others. These laws are intended to encourage individuals to pursue testing and treatment by providing patients with the assurance that their most sensitive health information will be treated with the highest degree of confidentiality. Additionally, most states developed common law whereby tort actions based on a theory of invasion of the right to privacy are used to redress wrongful disclosures of health information. However, levels of privacy protection continued to vary widely by state. By the 1990s, some states had broad, detailed privacy protections for health information while others offered few protections.[3]

II. The HIPAA Privacy Rule

As efforts to encourage the health care industry to adopt computer technology intensified, the need for federal standards to protect the privacy of health information became further apparent. In 1996, Congress addressed the issue of health information privacy within the context of the Health Insurance Portability and Accountability Act (HIPAA). The Administrative Simplification provisions of HIPAA were intended to encourage the development of an electronically based health care system. Congress gave itself a three-year deadline to enact comprehensive health privacy legislation designed to protect individuals' identifiable health information. As a fallback provision, if Congress failed to act within three years' time, the task of promulgating health privacy standards would shift to the U.S. Department of Health and Human Services (HHS). HIPAA expressly provides that if federal regulations are indeed promulgated, the federal mandates would not supersede a contrary provision of state law where the state standard is more stringent than that imposed by federal regulations.

Congress failed to pass comprehensive health privacy legislation within the self-imposed deadline. Some of the key stumbling blocks included hot-button privacy-related issues that continue to plague national policy debate, including reproductive rights and the treatment of minors' medical information, and tort reform issues of whether individuals should have the right to sue for wrongful disclosure of health information. When the 1999 deadline passed, in accord with HIPAA's requirements, the duty to craft federal health privacy protections passed to HHS.

In the waning days of President Clinton's second term, his administration issued the first version of the HIPAA Privacy Rule. The Bush administration allowed the rule to go into effect in 2003, only after making significant changes to the original rule. Under the current HIPAA Privacy Rule, with the exception of psychotherapy notes, all health information is handled in the same manner: it can be disclosed for treatment, payment, and

Under the current HIPAA Privacy Rule, with the exception of psychotherapy notes, all health information is handled in the same manner: it can be disclosed for treatment, payment, and health care operation purposes without first obtaining the individual's permission.

* Joy L. Pritts is a Research Associate Professor at the Health Policy Institute at Georgetown University.

health care operation purposes without first obtaining the individual's permission.[4] Although patients have the right to file complaints with HHS for violations of the Rule, they have no private right of action against the individual HIPAA violators.

Throughout the rule-making process, HHS consistently reiterated that it was establishing minimum federal standards which would not disturb more protective state laws. HHS explained that the Privacy Rule was "a new federal floor" establishing a set of basic consumer protections that states could choose to broaden or expand upon.[5] In short, the Privacy Rule was built on the understanding that it would serve as a minimal floor of protection and that state laws affording higher protections would be preserved.

As a result, many state laws still remain in effect today. Such laws afford heightened protections for sensitive medical information, particularly with regard to information related to genetic testing, HIV/AIDS, or mental health. Typically, states upholding more stringent standards will require that an individual's authorization or consent be obtained before this information may be shared beyond the originating health care provider. States also continue to enforce their own health privacy laws and afford their citizens the right to sue for improper disclosures of their privacy or to obtain their medical records.

III. Renewed Efforts to Preempt State Law

In 2004, the Bush administration released its outline of a ten-year plan to build a nationwide electronic health information infrastructure in the United States.[6] As this plan has progressed, there has been a renewed interest in wholly preempting state health privacy laws through new federal legislation. In 2005, the Healthcare Leadership Council, a coalition primarily comprised of health researchers and health industry executives from pharmaceutical and insurance companies, urged Congress to fully preempt state health privacy laws and to make the HIPAA Privacy Rule the single national health privacy standard.[7] Shortly thereafter, Representative Nancy Johnson (R-CT) introduced the Health Information Technology Promotion Act of 2005 (H.R. 4157), which seemed to pave the way for federal preemption.[8] H.R. 4157 required HHS to conduct a study of existing federal and state health information privacy laws and report to Congress with recommendations on how to "harmonize" the array of standards. According to the bill, if Congress failed to enact legislation based on the study's results within three years, HHS would then have the authority to propose a single set of federal standards preempting state health privacy laws. Essentially, H.R. 4157 permitted the preemption of state law by default. Though this provision proved to be extremely contentious and was removed from the final version of the bill passed by the House in September 2006, the separate authorization of the HHS study of state health privacy laws did remain.[9]

HHS explained that the Privacy Rule was "a new federal floor" establishing a set of basic consumer protections that states could choose to broaden or expand upon.

HHS's Agency for Healthcare Research and Quality has undertaken a nationwide project to assess and address the impact of organization-level business policies and state laws on security and privacy practices, and examine the degree to which they pose challenges to interoperable health information exchange.[10] Under the project, 33 states and one territory are to identify variations in state privacy practices and laws that represent "barriers" to health information exchange and then propose practical solutions to remedy the problems.[11] States were instructed that their recommendations could encompass changes in state and federal laws and regulations.[12] Privacy advocates have expressed concerns that the project could actually be used to encourage federal preemption of those state and local laws intended to protect the privacy of patients' medical records.[13] The established April 2007 deadline for states to issue their final reports summarizing the observed variations and proposed solutions is rapidly approaching.

IV. Future Prospects for Preemption

Even if current attempts to "harmonize" the diversity in state health privacy laws prove unsuccessful, efforts to fully preempt state health privacy laws are unlikely to subside any time in the near future. Many professionals in the health care industry have strong incentives to push for a single minimal federal health privacy standard. Allowing professionals to share all health information without first obtaining individual consent would undoubtedly be easier and less expensive than complying with current requirements.

Allowing professionals to share all health information without first obtaining individual consent would undoubtedly be easier and less expensive than complying with current requirements.

However, it remains questionable whether one federal standard for protecting health information is appropriate. First, states *are* different both in the health status of their populations and in their approaches to furthering public

health goals. The states have occupied the medical record/health information field for decades and continue to serve as laboratories for the development of this area of law. For example, California regulates online services that allow individuals to create their own personal health records. A number of states have begun requiring that notice be provided to affected individuals after a security breach of health information. Although the states have enacted legislation addressing these issues, currently there are no comparable federal statutes. Furthermore, some states are particularly strict with regard to the enforcement of privacy laws. For instance, a hospital in Oregon recently settled a state investigation into a large medical data breach by paying over $95,000 in costs and committing to spend millions more to provide one year of credit-protection services to all individuals whose records were stolen.[14] In contrast, at the federal level, HHS has not imposed a single dime in civil penalties to satisfy the more than 20,000 complaints of privacy infractions that have been reported to the agency.

The states have occupied the medical record/health information field for decades and continue to serve as laboratories for the development of this area of law.

Politically, it may be extremely difficult for Congress to fully preempt state health privacy laws. Polls have consistently shown that the privacy of health information is a major concern for the majority of Americans. Thus, it is unlikely that politicians would take a stance on the preemption issue that would leave them vulnerable to allegations of stripping citizens' state-endorsed privacy rights. In order to fully preempt state health privacy laws, Congress would first be required to agree on controversial issues, such as access to minors' health information. Hot-button issues such as this remain at least as divisive today as they were ten years ago, if not more so. Former Representative Johnson's original bill essentially conceded this point and called for the default preemption as a fallback measure designed to circumvent the lack of political consensus on the controversial issues. Lawmakers have nonetheless been reluctant to delegate their power over high profile issues in the manner she proposed.

V. Potential Solutions

States may agree to harmonize their laws in some less-controversial areas yet retain their traditional powers. For instance, states may successfully adopt uniform laws specifying the requisite content for disclosure consents or authorizations. Though changes in these areas would help to facilitate the interstate exchange of data, variation will likely remain in more substantive provisions, such as the requirement for specific authorization to disclose health information related to HIV/AIDS,

Technology may prove useful in resolving some of the difficulties posed by the need for interstate compliance with various state health privacy laws. Canada plans to include an automated policy negotiation service as part of its nationwide health information network.[15] Under Canada's proposed service, each regional health information system will encode its respective privacy policies and laws. When a system receives a request for data from another region, the two systems will interact to determine automatically whether the privacy laws of their respective jurisdictions permit the interstate transfer of the requested health data. This type of technology may help alleviate the perceived need for federal preemption of state law by resolving differences between state health privacy laws through computerized automation.

VI. Conclusion

Federal efforts to preempt all state health privacy laws will likely be unsuccessful anytime in the foreseeable future. Rather, it would be more effective to focus energy and efforts on encouraging states to harmonize their own laws where appropriate and to develop technology to accommodate differences where they continue to exist.

1 *See* John Pulley, Untying the Privacy Knot, Government Health It, Aug. 14, 2006, *available at* http://govhealthit.com/article95583-08-14-06-Print (last visited Feb. 12, 2007).
2 *See e.g.*, Mont. Code Ann. § 50-16-502 (2006).
3 *See* Joy Pritts, et. al, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 Yale J. Health Pol'y L. & Ethics 325, 327 (2002).
4 *See* Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.501 (Feb. 1, 2007) ("Psychotherapy notes" is narrowly defined as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record").
5 *See Preamble, Standards for Privacy of Individually Identifiable Health Information; Final Rule* (as modified), 67 Fed. Reg. 53, 212 (Aug. 14, 2002).
6 *See* Press Release, U.S. Dept. of Health and Human Services, Thompson Launches "Decade of Health Information Technology," (July 21, 2004), *available at* http://www.hhs.gov/news/press/2004pres/20040721a.html (last visited Feb. 12, 2007).
7 *See Health Information Technology: Hearing Before the H. Ways and Means Comm.*, 109th Cong. (2005) (statement of Mary R. Grealy, President, Healthcare Leadership Council), *available at* http://waysandmeans.house.gov/hearings.asp?formmode=view&id=2950 (last visited Feb. 12, 2007).

8 *See* Health Information Technology Promotion Act of 2005, H.R. 4157, 109th Cong. (2005-06).

9 *See generally Subcommittee on Health Report on H.R. 4157, The Health Information Technology Promotion Act of 2006* (June 13, 2006) (indicating that H.R. 4157 reported out of the Subcommittee on Health with the study on state laws intact, but without automatic preemption of state law if Congress failed to act). *But see* Chairman's Amendment in the Nature of a Substitute to H.R. 4157, The Health Information Technology Promotion Act of 2006, as reported by The Subcommittee on Health, *available at* http://waysandmeans.house.gov/Media/pdf/FC4157/4157SubcommitteeReport.pdf (last visited Feb. 12, 2007) *and* The Health Information Technology Promotion Act of 2006, H.R. 4157, 109th Cong. (June 13, 2006) (as reported by the Subcommittee on Health), *available at* http://waysandmeans.house.gov/Media/pdf/FC4157/HR4157asReported.pdf (last visited Feb. 12, 2007) (documenting that a variation of the provision was re-inserted in the Chairman's mark of the bill and was removed again before the bill ultimately was passed by the House).

10 *See Privacy and Security Solutions for Interoperable Health Information Exchange: Request for Proposals*, June 2005, Agency for Healthcare Research and Quality, Rockville, MD., http://www.ahrq.gov/fund/contarchive/rfp050015.htm (last visited Feb. 12, 2007).

11 *See id.* at 9.

12 *See* RTI International, *Transcript of Bidders' Conference Call,* Jan. 11, 2006 at 12. http://www.rti.org/files/Jan11BiddersCallTranscript.pdf (last visited Feb. 12, 2006).

13 *See Pulley*, *supra* note 1.

14 *See* Joe Rojas-Burke, *Providence Settles Data Breach*, The Oregonian, Sept. 27, 2006, at B1.

15 *See* Canada Health Infoway Inc., *Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture*, Version 1.1 (June 2005), *available at* http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security.pdf (last visited Feb. 12, 2007).

23